Lab - Forensic Analysis

Part I - Image Acquisition and Analysis

A tool called foremost can be used to view existing as well as deleted files. Remember that when we are carving, we only want to take a snapshot of the existing filesystem and not modify the current filesystem. You cannot run foremost on a mounted filesystem.

I have provided an image that I want you to look at.

<u>Image</u>

You should analyze the image and see what you find. You will also want to mount the iso. You can do this with the mount command and -o loop. As in mount -o loop file.img temp\ where temp is a directory that you have created and file.img is the file that you have downloaded.

Make a list of all jpg, pdf, wav, bmp files that you find. These files may have been deleted or may not, screenshot the image files as applicable. Put it in a single PDF document.

To Pass Off

Upload the PDF document of the above stuff by the required due date.